

APLIKASI ENKRIPSI DAN DESKRIPSI DATA MENGGUNAKAN ALGORITMA RC4 DENGAN MENGGUNAKAN BAHASA PEMROGRAMAN PHP

Elka Lukman Hakim, Khairil, Ferry Hari Utami

Program Studi Teknik Informatika Fakultas Ilmu Komputer Universitas Dehasen Bengkulu
Jl. Meranti Raya No. 32 Kota Bengkulu 38228 Telp. (0736) 22027, 26957 Fax. (0736) 341139

ABSTRACT

Security and confidentiality of data is currently a very important issue and continues to grow. Some cases involving data security is now a job that requires handling and security costs so much. To maintain the security and confidentiality of messages, data, or information that cannot be read or understood by any person, except for recipients who are entitled, then the application of a safety system designed by the method of data encryption using the RC4 algorithm. RC4 (Rivets Cipher 4) is a Synchrony stream cipher, which has a symmetric key cipher and encrypt the plaintext digits are digits per byte by byte or by combining with a binary operation XOR with a random number.

Keywords: Encryption, RC4, XOR Operation

INTISARI

Keamanan dan kerahasiaan data saat ini menjadi isu yang sangat penting dan terus berkembang. Beberapa kasus menyangkut keamanan data saat ini menjadi suatu pekerjaan yang membutuhkan biaya penanganan dan pengamanan yang sedemikian besar. Untuk menjaga keamanan dan kerahasiaan pesan, data, atau informasi agar tidak dapat di baca atau di mengerti oleh sembarang orang, kecuali untuk penerima yang berhak, maka dirancang aplikasi sistem pengaman data dengan metode enkripsi menggunakan algoritma rc4. RC4 (*Rivest Cipher 4*) adalah sebuah *synchron streamcipher*, yaitu *cipher* yang memiliki kunci simetris dan mengenkripsi *plainteks* secara digit per digit atau *byte* per *byte* dengan cara mengkombinasikan dengan operasi biner (biasanya *XOR*) dengan sebuah angka semi acak.

Kata Kunci : Enkripsi, RC4, XOR.

I. PENDAHULUAN

Di era globalisasi saat ini, mendapatkan informasi sangatlah mudah. Setiap orang dengan mudah mendapatkan data ataupun berita yang diinginkan. Hal ini didukung dengan teknologi informasi dan komunikasi yang berkembang pesat dari tahun ke tahun. Akan tetapi kemudahan mendapatkan informasi juga memberikan ancaman. Beberapa ancaman yang diberikan adalah masalah tentang keamanan, kerahasiaan, dan keotentikan data. Contohnya seperti password, data kerahasiaan perusahaan atau instansi.

Salah satu ilmu pengamanan data yang terkenal adalah kriptografi. Kriptografi adalah ilmu sekaligus seni untuk menjaga kerahasiaan pesan, data, atau informasi dengan cara menyamarkannya menjadi bentuk tersandi yang tidak mempunyai makna. Dalam kriptografi, terdapat 2 proses utama, enkripsi dan dekripsi. Enkripsi adalah proses penyandian pesan asli atau *plainteks* menjadi *cipherteks* (teks tersandi). Sedangkan dekripsi adalah proses penyandian kembali *cipherteks* menjadi *plainteks*.

Salah satu metode *enkripsi* yang terkenal adalah metode RC4. RC4 pertama kali dibuat oleh Ron Rivest di Laboratorium RSA pada tahun 1987. Awalnya RC4 adalah sebuah rahasia dagang, akan tapi pada September 1994, kode tersebut dikirim oleh seseorang yang tidak diketahui ke milist Chypermunks dan menyebar ke banyak situs internet. Kode yang bocor tersebut akhirnya dikonfirmasi

sebagai RC4 karena memiliki output yang sama dengan *software* dengan *license* RC4 di dalamnya. Karena algoritma sudah diketahui, RC4 tidak lagi menjadi rahasia dagang. Nama "RC4" sekarang adalah sebuah merek dagang, namun sering disebut sebagai "ARCFOUR" atau "ARC4" (artinya diduga RC4, karena algoritma ini tidak pernah dirilis secara resmi oleh RSA), untuk menghindari kemungkinan masalah tentang merek dagang.

RC4 (*Rivest Cipher 4*) adalah sebuah *synchron streamcipher*, yaitu *cipher* yang memiliki kunci simetris dan mengenkripsi *plainteks* secara digit per digit atau *byte* per *byte* dengan cara mengkombinasikan dengan operasi biner (biasanya *XOR*) dengan sebuah angka semiacak.

SMKS 08 Grakarsa Bengkulu merupakan Sekolah Menengah Kejuruan Swasta yang ada di Kota Bengkulu. Untuk keamanan datanya SMKS 08 Brakarsa B memerlukan sebuah sistem enkripsi data agar data tersebut terhindar dari campur tangan pihak ketiga yang dapat memanipulasi data tersebut. Oleh karena itu di SMKS 08 Grakarsa Bengkulu dirancang sebuah sistem kriptografi menggunakan algoritma RC4.

Berdasarkan uraian di atas, penulis tertarik untuk mengangkat judul penelitian yaitu "Program Enkripsi dan Deskripsi Data Menggunakan Algoritma RC4 dengan menggunakan Bahasa Pemrograman PHP".

Dari latar belakang diatas, dapat dirumuskan suatu masalah, yaitu bagaimana perancangan program

Enkripsi Data menggunakan Algoritma RC4 dengan menggunakan Bahasa Pemrograman PHP?

Batasan masalah dalam penelitian ini adalah perancangan program Enkripsi Data seperti data siswa, guru, keuangan dan lain-lain menggunakan Algoritma RC4 dengan menggunakan Bahasa Pemrograman PHP di SMKS 08 Grakarsa Bengkulu.

Penelitian ini memiliki tujuan Merancang perancangan program Enkripsi Data menggunakan Algoritma RC4 dengan menggunakan Bahasa Pemrograman PHP.

II. TINJAUAN PUSTAKA

A. Pengertian Algoritma dan Kriptografi

Menurut Setiadi (2000:12), algoritma adalah cara yang dapat ditempuh oleh komputer dalam mencapai suatu tujuan, terdiri atas langkah-langkah yang terdefinisi dengan baik, menerima *input*, melakukan proses dan menghasilkan *output*. Berikut ini adalah contoh menuliskan algoritma:

TUKAR ISI BEJANA;

Algoritma TUKAR_ISI_BEJANA

Diberikan dua buah bejana, A dan B. Bejana A berisi larutan berwarna merah, bejana B berisi larutan berwarna biru. Pertukarkan isi kedua bejana itu sedemikian sehingga bejana A berisi larutan berwarna biru dan bejana B berisi larutan merah.

Deskripsi:

- 1) Tuangkan larutan dari bejana A ke bejana C
- 2) Tuangkan larutan dari bejana B ke bejana A
- 3) Tuangkan larutan dari bejana C ke bejana B

Kriptografi secara umum adalah ilmu dan seni untuk menjaga kerahasiaan berita. Selain pengertian tersebut terdapat pula pengertian ilmu yang mengajarkan teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data (A. Menezes, P. Van Oorschot and S. Vanstone-Handbook of Applied Cryptography). Sedangkan menurut Kaufman et. al. (2002) menjelaskan bahwa kata Kriptografi berasal dari bahasa Yunani dan memiliki makna seni dalam menulis pesan rahasia (*The art of secret writing*), dimana kriptografi terdiri dari 2 kata yaitu *cryptós* yang berarti *rahasia* atau *tersembunyi* dan *gráphein* yang berarti *tulisan*. (Apriandala, 2013: 114).

Ada empat tujuan mendasar dari ilmu kriptografi ini juga merupakan aspek keamanan informasi yaitu Kerahasiaan adalah layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka/mengupas informasi yang telah disandi. Integritas data adalah berhubungan dengan penjagaan dari perubahan data secara tidak sah. Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi data oleh pihak-pihak yang tidak berhak, antara lain penyisipan,

penghapusan, dan substitusi data lain ke dalam data yang sebenarnya. Autentikasi adalah berhubungan dengan identifikasi/pengenalan, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Informasi yang dikirimkan melalui kanal harus diautentikasi keaslian isinya, waktu pengiriman dan lain-lain. Non-repudiasi atau penyangkalan adalah usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman/terciptanya suatu informasi oleh yang mengirimkan atau membuat.

Kriptografi memiliki 4 komponen utama yaitu:

- 1) *Plaintext*, yaitu pesan yang dapat dibaca.
- 2) *Ciphertext*, yaitu pesan sandi/pesan acak yang tidak bisa dibaca.
- 3) *Key*, yaitu kunci untuk melakukan teknik kriptografi.
- 4) *Algoritma*, yaitu metode untuk melakukan enkripsi dan dekripsi.

Proses-proses dasar kriptografi dibagi menjadi dua bagian, yaitu Enkripsi (*Encryption*) dan Dekripsi (*Decryption*).

Adapun contoh Teknik Kriptografi Klasik, yaitu:

- 1) Substitusi yaitu teknik ini mengganti satu atau sekumpulan bit pada blok *plaintexts* tanpa mengubah urutannya.
- 2) Transposisi yaitu teknik ini memindahkan posisi bit pada blok *plaintexts* berdasarkan aturan tertentu

Sedangkan contoh dari Teknik Kriptografi Modern sendiri yaitu:

- 1) Kriptografi Simetris, yaitu teknik enkripsi dan dekripsi dengan teknik atau metode atau kunci yang sama.
- 2) Kriptografi Asimetris, yaitu teknik enkripsi dan dekripsi dengan dua kunci yaitu kunci publik (*Public key*) dan kunci rahasia (*Private key*).
- 3) Kriptografi *Hibrid*, yaitu teknik enkripsi dan dekripsi dua lapis, maksudnya setelah file di enkripsi kemudian dilakukan enkripsi sekali lagi begitu sebaliknya.

B. Algoritma RC4

Menurut Andi (2007:25) Algoritma RC4 merupakan salah satu jenis *stream cipher*, yaitu memproses unit atau *input* data, pesan atau informasi pada satu saat. Unit atau data pada umumnya *sebuah byte* atau bahkan kadang-kadang bit (*byte* dalam hal RC4). Dengan cara ini enkripsi atau dekripsi dapat dilaksanakan pada panjang yang variabel. Algoritma ini tidak harus menunggu sejumlah *input* data, pesan atau informasi tertentu sebelum diproses, atau menambahkan *byte* tambahan untuk mengenkripsi. Contoh *stream cipher* adalah RC4, Seal, A5, Oryx, dan lain-lain. Tipe lainnya adalah *block cipher* yang memproses sekaligus sejumlah tertentu data,

biasanya 64 bit atau 128 bit blok, contohnya: Blowfish, DES, Gost, Idea, RC5, Safer, Square, Twofish, RC6, Loki97, dan lain-lain.

RC4 merupakan merupakan salah satu jenis *stream cipher*, yaitu memproses unit atau *input* data pada satu saat. Dengan cara ini enkripsi atau dekripsi dapat dilaksanakan pada panjang yang variabel. Algoritma ini tidak harus menunggu sejumlah *input* data tertentu sebelum diproses, atau menambahkan *byte* tambahan untuk mengenkrip. Metode enkripsi RC4 sangat cepat kurang lebih 10 kali lebih cepat dari DES.

Algoritma RC4 memiliki dua *fase*, setup kunci dan pengenkripsian. Setup untuk kunci adalah fase pertama dan yang paling sulit dalam algoritma ini. Dalam setup S- bit kunci (S merupakan panjang dari kunci), kunci enkripsi digunakan untuk menghasilkan variabel enkripsi yang menggunakan dua buah *array*, state dan kunci, dan sejumlah-S hasil dari operasi penggabungan. Operasi penggabungan ini terdiri dari pemindahan (*swapping*)byte, operasi modulo, dan rumus lain. Operasi modulo merupakan proses yang menghasilkan nilai sisa dari satu pembagian. Sebagai contoh, 11 dibagi 4 adalah 2 dengan sisa pembagian 3, begitu juga jika tujuh modulo empat maka akan dihasilkan nilai tiga.

III. METODOLOGI PENELITIAN

A. Subjek Penelitian

Subjek dari penelitian ini adalah SMKS 8 Grakarsa Kota Bengkulu yang beralamat di jalan Adam Malik KM 8 Kecamatan Gading Cempaka Kelurahan Lingkat Timur Kota Bengkulu.

B. Metode Penelitian

Metode penelitian yang digunakan dalam penelitian ini adalah metode pengembangan sistem. Adapun langkah-langkah penelitian adalah:

- 1) Analisis sistem aplikasi kriptografi pesan menggunakan algoritma Rivest Code 4 (RC4).
- 2) Implementasi dan pengujian sistem, yakni melakukan pengujian terhadap sistem yang telah dirancang.

C. Perangkat Lunak dan Perangkat Keras yang digunakan

Sistem perangkat lunak merupakan program pendukung yang diperlukan dalam menjalankan perangkat keras. *Software* sebagai penerjemah suatu bahasa mesin (*analog*) yang menghasilkan informasi yang dapat dikenal oleh manusia. Adapun perangkat lunak yang mendukung program ini adalah:

- 1) Sistem Operasi: Windows 7
- 2) Program Aplikasi: Bahasa Pemrograman PHP.

Perangkat keras merupakan suatu peralatan fisik komputer yang digunakan untuk menjalankan program yaitu :

- 1) Monitor 14" WXGA WideScreen
- 2) Prosesor Intel Centrino M-16
- 3) Ram 1024 MB

D. Analisa Sistem

Untuk menunjukkan algoritma RC4 bekerja pada tingkat dasar, maka dicontohkan dengan state-array 4 bit. Hal ini dikarenakan akan sangat sulit menggambarkan proses RC4 secara manual dengan state-array 256 bit. Kali ini, kita akan mengenkripsi kata SAYA SENANG dengan kunci 2573.

Pertama, kita menginisialisasi array S 4 bit dengan memblok kalimat "SAYASENANG". Terlebih dahulu kalimat tersebut dibagi menjadi 4 block dan apabila terjadi kekurangan dari block ditambah dengan huruf X. Hal tersebut berguna untuk mempersulit analisis dari cipher tersebut.

Setelah membagi kalimat tersebut menjadi 4 byte maka terbentuk *state-array* S dan *state-array* K sebagai berikut:

Array S			
0	1	2	3
2	5	7	3

Inisialisasi i dan j dengan 0 kemudian dilakukan KSA agar tercipta *state-array* yang acak. Penjelasan iterasi lebih lanjut dapat dijelaskan sebagai berikut.

0

$$J = (0 + S[0] + K[0 \bmod 4]) \bmod 4 \\ = (0 + 0 + 2) \bmod 4 = 2$$

Swap (S[0], S[2])

Hasil Array S			
2	1	0	3

Iterasi 2

$$i = 1 \\ j = (2 + S[1] + K[1 \bmod 4]) \bmod 4 \\ = (2 + 1 + 5) \bmod 4 = 0$$

Swap (S[1], S[0])

Hasil Array S			
1	2	0	3

Iterasi 3

$$i = 2 \\ j = (0 + S[2] + K[2 \bmod 4]) \bmod 4 \\ = (0 + 0 + 7) \bmod 4 = 3$$

Swap (S[2], S[3])

Hasil:			
1	2	3	0

Iterasi 4

$i = 3$

$$j = (3 + S[3] + K[3 \bmod 4]) \bmod 4 \\ = (3 + 0 + 3) \bmod 4 = 2$$

Swap ($S[3], S[2]$)

Hasil Array S

1	2	0	3
---	---	---	---

Setelah melakukan KSA, akan dilakukan PRGA. PRGA akan dilakukan sebanyak 4 kali dikarenakan plainteks yang akan dienkripsi berjumlah 4 karakter. Hal ini disebabkan karena dibutuhkan 1 kunci dan 1 kali pengoperasian XOR untuk tiap-tiap karakter pada plainteks. Berikut adalah tahapan penghasilan kunci enkripsi dengan PRGA.

Array S

1	2	0	3
---	---	---	---

Iterasi 1

$$i = (0 + 1) \bmod 4 = 1$$

$$j = (0 + S[1]) \bmod 4 = (0 + 2) \bmod 4 = 2$$

Swap ($S[1], S[2]$)

Hasil

1	0	2	3
---	---	---	---

$$K1 = S[(S[1] + S[2]) \bmod 4] = S[2 \bmod 4] = 2 \\ K1 = 00000010$$

Iterasi 2

$$i = (1 + 1) \bmod 4 = 2$$

$$j = (2 + S[2]) \bmod 4 = (2 + 2) \bmod 4 = 0$$

Swap ($S[2], S[0]$)

Hasil

2	0	1	3
---	---	---	---

$$K2 = S[(S[2] + S[0]) \bmod 4] = 1 \\ K2 = 00000011$$

Iterasi 3

$$i = (2 + 1) \bmod 4 = 3$$

$$j = (0 + S[3]) \bmod 4 = (0 + 3) \bmod 4 = 3$$

Swap ($S[3], S[3]$)

Hasil

1	0	2	3
---	---	---	---

$$K3 = S[(S[3] + S[3]) \bmod 4] = S[6 \bmod 4] = 2 \\ K3 = 00000010$$

Iterasi 4

$$i = (3 + 1) \bmod 4 = 0$$

$$j = (3 + S[0]) \bmod 4 = (3 + 1) \bmod 4 = 0$$

Swap ($S[0], S[0]$)

Hasil

1	0	2	3
---	---	---	---

$$K3 = S[(S[0] + S[0]) \bmod 4] = S[2 \bmod 4] = 2 \\ K3 = 00000010$$

Setelah menemukan kunci untuk tiap karakter, maka dilakukan operasi XOR antara karakter pada *plaintext* dengan kunci yang dihasilkan.

IV. PEMBAHASAN

A. Hasil Program dan Pembahasan

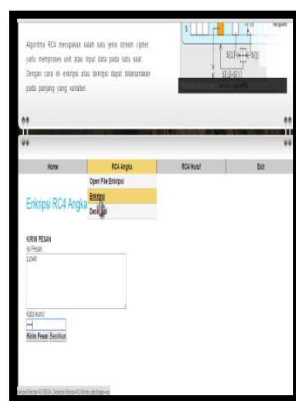
Tampilan Halaman Home: Halaman ini merupakan tampilan awal sistem. Pada halaman ini disediakan informasi mengenai algoritma RC 4. Adapun tampilan halaman home dapat dilihat pada Gambar 1.



Gambar 1 Tampilan Halaman Home

Tampilan Halaman RC4 Angka Open File RC4 Angka: Pada halaman ini terdapat *form* yang disediakan untuk memasukkan file angka yang berformat *.txt* ke dalam sistem. Sehingga data tersebut dapat dienkripsi dan deskripsi. Adapun tampilan halaman *open file* angka dapat dilihat pada Gambar 2.

Tampilan Halaman Enkripsi RC4 Angka: Halaman ini digunakan untuk mengenkripsi data angka dengan memasukkan angka yang akan dienkripsi ke dalam kotak kosong yang telah disediakan, kemudian masukkan kunci enkripsi minimal 5 karakter. Setelah itu klik "kirim". Tampilan halaman enkripsi dapat dilihat pada Gambar 3.

Gambar 2 Tampilan Halaman *Open File Angka*

Gambar 3. Tampilan Halaman Enkripsi RC4 Angka

Tampilan Halaman Deskripsi RC4 Angka: Halaman ini digunakan untuk mendeskripsi data angka dengan memasukkan kata kunci pada saat enkripsi data sebelumnya. Tampilan halaman deskripsi data angka dapat dilihat pada Gambar 4.



Gambar 4 Tampilan Halaman Deskripsi RC4 Angka

Setelah kata kunci dimasukkan, maka data akan dideskripsi sehingga hasilnya kembali ke *Plaintext*. Seperti pada Gambar 5.

Tampilan Halaman Open File RC4 Huruf: Pada halaman ini terdapat *form* yang disediakan untuk memasukkan *file* huruf yang berformat *.txt* ke sistem. Sehingga data tersebut dapat dienkripsi dan deskripsi.

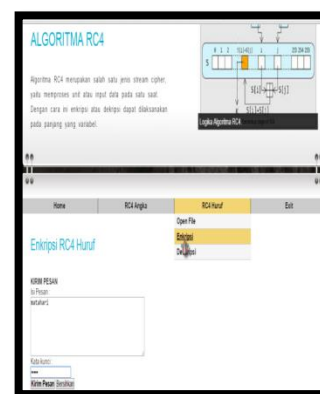
Adapun tampilan halaman *open file* huruf dapat dilihat pada Gambar 6.



Gambar 5. Tampilan Halaman Hasil Deskripsi RC4 Angka

Gambar 6. Tampilan Halaman *Open File* RC4 Huruf

Tampilan Halaman Enkripsi RC4 Huruf: Halaman ini digunakan untuk mengenkripsi data huruf dengan memasukkan huruf yang akan dienkripsi ke dalam kotak kosong yang telah disediakan, kemudian masukkan kunci enkripsi minimal 5 karakter. Setelah itu klik "kirim". Tampilan halaman enkripsi huruf dapat dilihat pada Gambar 7.



Gambar 7 Tampilan Halaman Enkripsi RC4 Huruf

Tampilan Halaman Deskripsi RC4 Huruf:
Halaman ini digunakan untuk mendeskripsi data huruf dengan memasukkan kata kunci pada saat enkripsi data sebelumnya. Tampilan halaman deskripsi data huruf dapat dilihat pada Gambar 8.

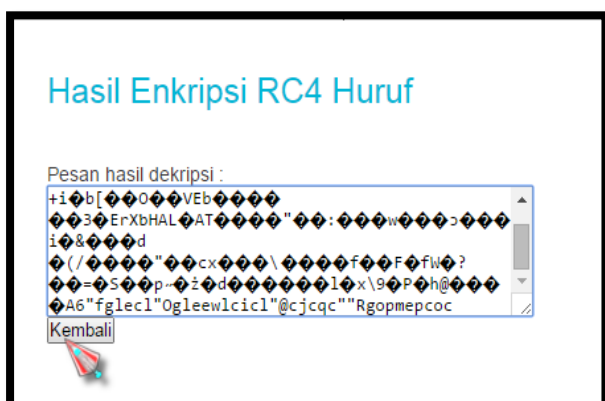


Gambar 8. Tampilan Halaman Deskripsi RC4 huruf

4.2 Hasil Pengujian

Pengujian system enkripsi dan deskripsi data menggunakan Algoritma RC4 dengan menggunakan bahasa pemrograman PHP pada SMA Grakarsa Kota Bengkulu dilakukan di depan Kepala sekolah SMKS 8 Grakarsa B Kota Bengkulu dengan maksud untuk menguji kelayakan sistem yang dibuat dan untuk mengetahui kelemahan dari sistem yang dibuat sehingga serta dapat dievaluasi atau diperbaiki. Selain kepada kepala sekolah SMKS 8 Grakarsa B Kota Bengkulu, pengujian sistem juga dilakukan kepada 3 orang orang guru, yaitu dengan membuat kuisioner dari system enkripsi dan deskripsi data menggunakan Algoritma RC4 dengan Menggunakan Bahasa Pemrograman PHP. Dari hasil pengujian yang dilakukan maka dapat disimpulkan bahwasanya sistem enkripsi dan deskripsi data menggunakan Algoritma RC4 dengan Menggunakan Bahasa Pemrograman PHP dapat mempermudah dalam mengubah data ke dalam bentuk yang tidak dapat dimengerti oleh orang lain, sehingga kerahasiaan data dapat dijaga.

Adapun hasil pengujian sistem yang dilakukan adalah sebagai berikut.



Berdasarkan hasil pengujian di atas, maka dapat disimpulkan sistem enkripsi dan deskripsi data menggunakan algoritma RC4 dapat mengubah angka dan huruf ke dalam bentuk yang tidak ada arti dan tidak dapat dimengerti.

V. PENUTUP

A. Kesimpulan

Dari hasil dan pembahasan serta pengujian sistem maka dapat diambil beberapa kesimpulan, yaitu:

- 1) Bahasa pemrograman PHP dapat memberikan kemudahan dalam pembuatan enkripsi dan deskripsi data menggunakan Algoritma RC4 pada SMA Grakarsa Kota Bengkulu
- 2) Pembuatan sistem enkripsi dan deskripsi data menggunakan Algoritma RC4 dengan menggunakan bahasa pemrograman PHP pada SMA Grakarsa Kota Bengkulu dapat memberikan kemudahan dalam proses enkripsi data sehingga dapat menjaga kerahasiaan data.

B. Saran

Agar sistem yang diusulkan dapat digunakan lebih optimal dan dapat berjalan sesuai dengan yang diharapkan, maka ada beberapa saran yang dapat dijadikan bahan pertimbangan untuk pihak SMA Grakarsa Kota Bengkulu, yaitu:

- 1) Sistem yang dibangun pada intinya hanya sebatas sistem enkripsi dan deskripsi data menggunakan Algoritma RC4 dengan menggunakan bahasa pemrograman PHP pada SMA Grakarsa Kota Bengkulu. Sehingga kedepannya diharapkan adanya pengembangan lagi untuk sistem yang lebih luas cakupannya seperti pengujian sistem secara online dan lain sebagainya.
- 2) Diperlukan *maintenance* terhadap sistem yang telah dibuat, supaya dapat digunakan secara berkelanjutan selama kebutuhan terhadap informasi yang dibutuhkan.

DAFTAR PUSTAKA

- Apriandala, Rio, 2013, *Sistem Keamanan Menggunakan Rubik Dengan Algoritma Kriptografi Encryption*, Tugas Besar I Makalah Kriptografi, Universitas Bengkulu. 375 Hal.
- Ems, TIM. 2012. *Web Progreming for Beginners*. Jakarta: PT Elex Media Komputindo.
- Jogiyanto, HM. 2011. *Pengenalan Komputer, Dasar Ilmu Komputer, Pemrograman*, Salemba Empat: Yokyakarta.
- Kristianto, Andi, *Keamanan Data*, Gava Media, Yogyakarta, 2003.
- Mulyono, Sigit. 2008. *Perancangan Image Vektor Dengan Adobe Illustrator*. UNIKOM. Bandung: Bumi Aksara.
- Nugroho, Bunafit. 2011. *Sistem Informasi Penjualan Berbasis Web dengan PHP dan MySQL*. Yokyakarta: Gava Media.
- Yakub, 2012 *Pengantar Sistem Informasi*, Yogyakarta, Graha Ilmu. 155.